UNITED STATES DEPARTMENT OF AGRICULTURE
FOOD SAFETY AND INSPECTION SERVICE
WASHINGTON, DC

# FSIS DIRECTIVE	5420.4, Revision 5	11/17/08

HOMELAND SECURITY THREAT CONDITION RESPONSE - EMERGENCY PROCEDURES FOR THE OFFICE OF INTERNATIONAL AFFAIRS IMPORT INSPECTION DIVISION

I. PURPOSE

A. This directive details the procedures that Import Inspection Division (IID), Office of International Affairs (OIA), Food Safety and Inspection Service (FSIS), field personnel are to follow when the Department of Homeland Security declares a threat condition Yellow, Orange, or Red.

B. This directive also:

- establishes how threat condition declarations are to be communicated to import inspection personnel;

- provides specific instructions to import inspection personnel on how to record any findings and respond to threat condition declarations;

- provides procedures for informing OIA supervisors, the Office of Food Defense and Emergency Response (OFDER), and border personnel from other agencies of security concerns;

- provides procedures to effectively address and resolve noted security concerns in order to ensure that food is protected, thereby protecting public health; and

- provides instruction for import inspection personnel when checking to see if a facility (official establishment, in-commerce facility, or port-of-entry) has a food defense plan.

C. If there is an actual terrorist attack on a port of entry (POE), import personnel will immediately take measures to make sure program personnel are safe and are to notify the Regional Import Field Office (RIFO). The RIFO will then notify IID Headquarters and the appropriate local authorities. In addition, the RIFO may request the activation of the FSIS Emergency Management Committee (EMC) through the senior executive leadership in OIA (see FSIS Directive 5500.2, Significant Incident Response).

II. CANCELLATION

FSIS Directive 5420.4, Revision 4, Homeland Security Threat Condition Response – Emergency Procedures for the Office of International Affairs Import Inspection Division, dated 1/7/08.

III. REASON FOR REISSUANCE

FSIS is reissuing this directive in its entirety to incorporate instructions for documenting food defense surveillance findings in the In-Commerce System (ICS). Findings are to no longer be documented in the SharePoint site. This issuance also provides clarification related to the frequency for conducting food defense surveillance procedures and describes how the data generated from the procedures is used.

IV. REFERENCES

9 CFR parts 300 to end
FSIS Directive 5420.1, Rev. 4, Homeland Security Threat Condition Response – Food Defense Verification Procedures
FSIS Directive 5420.3, Rev. 5, Homeland Security Threat Condition Response – Surveillance of Firms, Establishments and Products in Commerce
FSIS Directive 5500.2, Significant Incident Response
Homeland Security Presidential Directive/HSPD-9, Subject: Defense of United States Agriculture and Food
Public Health Security and Bioterrorism Act of 2002, Section 332 (21 USC 679C)

V. BACKGROUND

In 2002, the White House Office of Homeland Security established a Homeland Security Advisory System based on color. This System provides a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. A declaration of a Threat Condition Elevated (Yellow) by the Department of Homeland Security indicates that there is an elevated risk of terrorist attacks. A declaration of a Threat Condition High (Orange) indicates there is a high risk of terrorist attacks. A declaration of a Threat Condition Severe (Red) reflects a severe risk of terrorist attacks. While the threat may or may not involve the nation's food supply, it is imperative that Agency personnel take certain actions immediately during such threat conditions to ensure the safety of meat, poultry, and egg products. Given what is required in responding to a credible threat of a terrorist attack, FSIS personnel must clearly understand their roles and what will be required of them in order to respond properly to that threat.

VI. NOTIFICATION

A. In the event of a declaration of any threat condition:

- Elevated (Yellow), when there is an elevated risk of terrorist attacks,
- High (Orange), when there is a high risk of terrorist attacks, or
- Severe (Red) when there is a severe risk of terrorist attacks,

by the Department of Homeland Security, FSIS' OFDER is to inform the FSIS Administrator and FSIS Management Council. OFDER is to issue an e-mail letter to all employees notifying them of the heightened threat condition.

B. The RIFO is to notify import field personnel at the time of the declaration to conduct Food Defense Verification Procedures for the threat condition according to the activities set forth in Paragraphs IX and X of this directive. The import inspector is to notify the import facility management of the threat condition and of the implementation of the Food Defense Verification Procedures.

C. Import Surveillance Liaison Officers (ISLOs) will maintain communications with the Department of Homeland Security (Customs and Border Protection (CBP), Coast Guard), Food and Drug Administration (FDA), Animal and Plant Health Inspection Service (APHIS), other agencies, and other FSIS personnel at POE and are to initiate the appropriate Food Defense Verification Procedures outlined in Section X of this directive.

D. OFDER is to communicate the downgrading of a threat condition to the FSIS Administrator and the FSIS Management Council. Upon notification from OIA senior executive leadership, the RIFO is to notify import field inspection personnel of the downgrade. The RIFO is to notify import establishments that the downgrading has taken place.

VII. SPECIFIC THREAT CONDITION ACTIVITIES

The following are the actions to take in the event of a declaration of:

A. Threat Condition Elevated (Yellow), High (Orange), or Severe (Red) with no specific threat to the food and agricultural sector

1. The RIFO is to:

a. brief IID management on all food defense field activities and communicate any immediate concerns to OIA senior executive leadership;

b. confirm that import inspection program personnel are aware of any changes in threat conditions, and that they have conveyed the current threat condition to management of import establishments;

c. verify that import inspectors perform Food Defense Verification Procedure (Import Inspectors) and ISLO's perform Food Defense Surveillance Activities;

d. monitor import establishment and border activity; and

e. coordinate any food security activities with other border agencies as assigned by IID Headquarters.

2. Import inspectors are to:

a. continue to consult the Automated Import Information System (AIIS) for reinspection assignments. Should the AIIS become inaccessible, import inspectors should follow the Import Manual of Procedures, Part 1, Section 1, until receiving alternative instruction;

b. initiate Food Defense Verification Procedures through PBIS (refer to paragraph IX of this directive) and perform one randomly selected Food Defense Verification Procedure (Inspection System Procedures (ISP) Codes O8S14 through O8S17) daily at active import establishments for the duration of the threat condition; and

c. perform and record the Food Defense Verification Procedures (ISP Codes O8S14 through O8S17) as UNSCHEDULED procedures within the established tour of duty and after all other PBIS procedures are completed.

3. ISLOs are to:

a. maintain communications with the DHS-CBP, the Coast Guard, FDA, APHIS, other agencies, and other FSIS personnel at POE within their jurisdiction;

b. report any irregularities, including suspicious behavior, and any alerts conveyed by other border agencies to OIA through supervisory channels;

c. coordinate any verification activities at a POE where an ISLO is not present;

d. implement Food Defense Surveillance Activities as specified in Section X;

e. notify the import establishments, warehouses attached to import establishments or located within the port of entry, or bonded warehouses about the change of the alert status.

B. Threat Condition High (Orange) with a specific threat to the food and agricultural sector.

1. The RIFO is to:

a. communicate heightened alert status and updates to all import field personnel at POEs;

b. conduct regular briefings with headquarters and field personnel; and

c. ensure import field personnel receive and implement any special instructions from OIA regarding the reinspection of suspect shipments.

2. Import Inspectors are to:

a. perform randomly three of the Food Defense Verification Procedures (ISP Codes O8S14, O8S15, O8S16, and O8S17) daily at active import establishments for the duration of the threat condition;

b. notify the RIFO or ISLO if the AIIS is down, and the contingency plan is in use; and

c. follow any special instructions provided by the RIFO regarding the reinspection of suspect shipments.

3. The ISLOs are to:

a. review high-risk product/shipments identified at POE as suspicious, including using radiation detectors on suspect shipments;

b. coordinate Homeland Security activities in coordination with other border agencies, as well as other FSIS activities, as directed by OIA; and

c. represent FSIS through attendance at POE Homeland Security Meetings and Pest Risk Committees, providing reports as necessary to OIA senior level management.

C. Threat Condition Severe (Red) with a specific threat to the food and agricultural sector.

1. The RIFO is to:

a. implement increased sampling at POE or import establishments for all or targeted (e.g., high-risk product) shipments as directed by OIA, in coordination with CBP;

b. in the event of a border/port of entry closing, notify OIA Headquarters and instruct import inspection personnel to hold all products that have been presented to FSIS; and

c. verify the removal of all import inspection program personnel from any threatening situation and notify OFDER through the senior executive leadership in OIA using the procedures as listed in FSIS Directive 5500.2, Non-Routine Incident Response.

2. The import inspector is to:

a. perform all Food Defense Verification Procedures (ISP Codes O8S14, O8S15, O8S16, and O8S17) daily for the duration of the threat condition;

b. increase scrutiny of all shipments, closely observing shipments to detect any evidence of tampering or to identify anything that is “suspicious;”

c. hold shipments as directed by the RIFO;

d. follow sampling instructions through AIIS. If the AIIS is non-operational, perform 100 percent reinspection of products. If radiation pagers are available, scan shipments for possible contaminants; and

e. conduct any unscheduled Food Defense types of inspections (TOIs) as assigned by the RIFO or IID management.

3. The ISLO is to:

a. respond to specific incidents within his/her jurisdiction;

b. initiate and coordinate emergency response activities through the RIFO across all jurisdictions; and

c. coordinate POE targeted shipment verification or FSIS sampling activities with import inspection personnel and CBP and facilitate any tests conducted on the shipment at POE with CBP.

D. Imported Egg Products

IID Headquarters is to direct all imported egg shipments to an official import establishment during Threat Condition High (Orange) or Severe (Red), with a specific threat to the food and agricultural sector. Import inspectors are to follow procedures in Paragraph IX and:

a. review shipment documentation;

b. observe shipment condition from shipping dock;

c. hold all suspicious shipments; and

d. contact RIFO for further instructions.

E. Targeted Shipments

Import inspectors are to reinspect shipments targeted as a food security risk per OIA regardless of the alert condition. Import inspectors are to maintain communication with the RIFO or headquarters. Reinspection may include:

a. review of shipment documentation;

b. food Security Lab sampling;

c. reinspection for tampering or adulteration;

d. radiation scanning, or

e. use of sensory equipment to detect biological or chemical contamination.

VIII. FOOD DEFENSE PLAN

A. Although not explicitly required by FSIS statute or regulation, FSIS has urged official establishments, in-commerce facilities, and bonded establishments located at ports-of-entry to develop functional food defense plans to set out control measures to prevent intentional adulteration of product. Although not required, FSIS considers these plans to be important preparatory measures. The plan should be developed, written, implemented, assessed, and maintained if it is to be functional. The Agency has developed guidelines on the elements of a food defense plan. They are available on the FSIS Web site at http://www.fsis.usda.gov/pdf/Elements_of_a_Food_Defense_Plan.pdf.

B. Management at official establishments, in-commerce facilities, and bonded establishments at ports-of-entry are not obligated to share a copy of the written plan to FSIS program personnel. If an establishment does share the plan, FSIS personnel should only use the plan to help them readily identify how the official establishment, in-commerce facility, or the bonded establishment at a port-of-entry is addressing food defense. If these facilities are not implementing elements of its plan, FSIS personnel cannot take action on that fact because there are no requirements for such plans. FSIS personnel are not to show or share the plan with any outside source because it may contain sensitive security information.

Import Inspector NOTE: When official establishment (I-House) management develops and implements a new food defense plan, or when management revises an existing food defense plan, Import Inspectors are to update the responses to the food defense profile extension in PBIS.

ISLO NOTE: When management of in-commerce facilities or bonded establishments at ports-of-entry develop and implement a new food defense plan, or when management revises an existing food defense plan, ISLOs are to reference this under Block 9 of FSIS Form 5420-3 when they re-visit the facility or port-of-entry.

IX. FOOD DEFENSE VERIFICATION PROCEDURES – Import Inspectors

A. The purpose of the following emergency Food Defense Verification Procedures is to identify and mitigate to the maximum extent possible potential vulnerabilities in imported meat, poultry, or egg products. A potential vulnerability can be any part of the food continuum system identified at the import facility or POE where a measure should be implemented to protect facility or POE operations. Examples include suspicious activity or evidence of tampering (holes or cuts in packages) in imported products.

B. Import Inspectors are to:

1. notify the facility management of any observation or concern;

2. take immediate action as per established policy any time they observe product adulteration;

3. monitor establishment operations for any unusual activity that may be related to food defense;

4. report any observations or suspicious activity related to food defense to their supervisor, the establishment, and the ISLO;

5. initiate Food Defense Verification Procedures through PBIS (ISP Codes 08S14 through 08S17).

NOTE: While conducting Food Defense Verification Procedures, import inspectors are to observe all areas of the import facility, including interior and exterior areas of the warehouse that may extend beyond the designated part of the official import establishment. If the import inspector identifies vulnerabilities, the inspector is to notify plant management, contact the RIFO and the ISLO, and document the vulnerabilities as set forth in this directive.

C. **O8 Procedures**

1. Water systems – 08S14

Observe the security of the facility's water systems, especially well water, ice production and storage facilities, and water reuse systems. Pay special attention to water used in defrost tanks and for purposes of cleaning and disinfecting.

Suggested Activities:

- Determine whether access to private wells is controlled.
- Determine whether potable water lines or storage tanks are appropriately secured.
- Determine whether ice production and storage facilities are appropriately secured.

2. Processing/Manufacturing – 08S15

Observe import reinspection process (raw and processed product handling, repackaging of product) where exposed products are being handled for indications of attempts to introduce contaminants into the product. Observe whether the facility has procedures in place to prevent deliberate contamination (e.g., camera surveillance, or restricted access of personnel to sensitive production or reinspection areas).

Suggested Activities:

- Check the import reinspection process (e.g. exposing of product for sampling) for evidence of possible intentional product contamination.
- Check to determine whether the establishment has implemented a system to restrict access to areas where reinspection is occurring (e.g., camera surveillance, color-coded uniforms, identification badges, sign out sheets).

3. Storage Areas – 08S16

Observe products in cold and dry storage areas for evidence of tampering. Pay special attention to bulk product ingredients, such as combo bins of meat trim and poultry parts used for grinding or emulsification. Dry ingredients, including spices, breading materials, and those used in injection solution preparations, also should be checked for indication of tampering. Observe the use and storage of any hazardous materials in the establishment including ingredients such as nitrites. Verify that entry into such storage areas is controlled, and that usage logs are maintained and current. Special attention should be paid to cleaning materials, particularly those used in clean-in-place systems, or where there is mixing of bulk products (e.g., storage silos). In addition, verify the control of laboratory reagents and cultures.

Suggested Activities:

Verify that the facility has implemented:

- Access control procedures to dry ingredient areas.
- Access control procedures to raw product storage areas.
- Access control procedures to finished product storage areas.
- Observation of all products in storage for evidence of tampering.
- Control procedures for access and use of hazardous chemicals.

4. Shipping and Receiving – 08S17

Observe loading dock areas and vehicular traffic in and out of the facility. Report all unattended deliveries on loading docks and unmarked vehicles parked on the premises to facility management immediately. Suggest that facility management secure dry and cold products stored in on-site trailers; that the trailers be parked in restricted access areas of the facility where possible; and that facility security staff routinely check the trailers' physical integrity (e.g. locks, seals, general condition). Pay special attention to deliveries of liquid egg products to storage silos, of combo bins of meat trim, and of dry ingredients.

Suggested Activities:

- Check to determine whether the facility has procedures in place to restrict or control access to the loading dock area, and verify that it is implementing these access control procedures.
- Observe incoming shipments to verify that the facility is checking deliveries against shipping documents. Special attention should be paid to tanker trucks and totes of liquid egg products; dry ingredients; combo bins of fresh meat trim or poultry parts; and boxes of frozen trim that are to be further processed.
- Observe outdoor lighting and on-site trailer security, paying special attention to any unauthorized access.

X. FOOD DEFENSE SURVEILLANCE PROCEDURES - ISLOs

A. ISLOs conduct surveillance reviews at warehouses, distributors, and other in-commerce facilities and at ports-of-entry to verify that persons and firms, whose business activities involve FSIS-regulated products, prepare, store, transport, sell, or offer for sale or transportation such products in compliance with FSIS statutory and regulatory requirements. These surveillance reviews include procedures for food defense surveillance as well as for food safety of imported products.

B. ISLOs conduct food defense surveillance procedures to identify potential security vulnerabilities at in-commerce facilities and ports-of-entry that increase the risk of intentionally adulterated meat, poultry, and egg products. A potential vulnerability can be any part of the food continuum system identified at the facility or port-of-entry where measures can be taken to protect food products from intentional product tampering adulteration. Examples of potential vulnerabilities include:

- unrestricted access to product storage and staging areas;
- unrestricted access to product processing areas;
- unrestricted access to shipping/receiving areas; or
- unrestricted access to water systems.

C. When ISLOs conduct food defense surveillance procedures they are to:

1. Food Defense Plan – determine whether the facility (e.g., warehouse, distribution center) has the following:

a. a written food defense plan that consists of standard operating procedures for preventing intentional product tampering and adulteration; and

b. contact information to be used if product is intentionally adulterated, e.g., police, state and local health agencies.

2. Outside Security – determine whether the facility has a means to protect the outer perimeter of the facility, such as a surveillance system (e.g., cameras, security guards, lighting, alarm system, locks) to secure the facility and outside premises.

3. Inside Security – observe and determine whether the facility has:

a. a surveillance system (e.g., cameras, security guards, lighting, alarm system, locks) to secure the inside premises.

b. measures in place to ensure that all persons (e.g., employees, contractors, construction or maintenance personnel) in the facility are authorized, properly identified, and restricted from areas as appropriate;

c. a process for the use, storage and controlled access of hazardous materials in the facility to prevent product adulteration; and

d. a process to protect food and food ingredients, including water used in

products prepared by the facility especially if it is well water. Note: this question applies to facilities that store products only, e.g., distributors and warehouses AND facilities that process products, e.g.; retail stores and restaurants.

4. Receiving/Shipping – observe and determine whether the facility or port-of-entry has:

a. a process that restricts access to the receiving/shipping areas to authorized personnel;

b. a process to verify that incoming/shipped products are consistent with shipping documents;

c. a process to examine all incoming products for indications of apparent tampering or adulteration (e.g., opened or resealed boxes, the presence of an unidentified substance on packaging or product, or questionable products, packaging or labeling); and

d. a process for maintaining security of products during loading/shipping, (e.g., trucks and trailers are locked or sealed while not under the direct supervision of company personnel).

5. Product Observation – determine whether there are any indications for products currently held in storage by the facility or port-of-entry of apparent product tampering or adulteration.

D. ISLOs are to conduct food defense surveillance procedures when a facility is reviewed for the first time or during follow-up surveillance where food defense surveillance procedures were not conducted within the previous 12 months.

XI. FOOD DEFENSE VERIFICATION PROCEDURE DOCUMENTATION - ISLOs

A. ISLOs are to conduct the food defense surveillance procedures listed in paragraph X above at threat condition Elevated (Yellow) or higher and are to document the findings in the In-Commerce System (ICS).

B. If ISLOs find food defense vulnerabilities, they are to provide a printed hard copy of the completed FSIS Form 5420-3 to the management at the time of the visit or subsequently send a copy to the facility management by fax or regular mail.

NOTE: FSIS Form 5420-3 is to be completed and printed using the ICS. The form can also be found in Outlook:\\Public Folders\All Public Folders\Agency Issuances\Forms\FSIS 5,000 Series.

C. ISLOs may not have access to ICS while conducting the food defense surveillance procedures. ISLOs are to document findings on FSIS Form 5420-3 and enter the information from the Form into ICS as soon as possible.

D. OIA supervisors and managers, as well as other OPEER and OFDER personnel have access to the data entered by ISLOs, in addition to having access to summary reports of the data in the ICS application.

E. ISLOs are to follow the established policy described in FSIS Directive 8410.1, Detention and Seizure, when they have reason to believe that meat, poultry, or egg products in commerce are adulterated, misbranded, or otherwise in violation of the Federal Meat Inspection Act, (21 U.S.C. 672), Poultry Products Inspection Act, (21 U.S.C. 467a) or the Egg Products Inspection Act, (21 U.S.C. 1048).

F. ISLOs are to follow procedures defined in FSIS Directive 5500.2, Non-Routine Incident Response, when they have evidence or information that indicates product may have been tampered with or other findings that may require an NRIR.

XII. FOOD DEFENSE DOCUMENTATION – IMPORT INSPECTORS

A. Import inspectors are to record the performance of the ISP procedures listed in paragraph IX and document findings in the following manner:

1. When import inspectors perform an 08S procedure and do not find a food defense vulnerability or concern, they are to record the procedure as performed by recording trend indicator “A”.

2. When import inspectors perform an 08S procedure and find that there is a food defense vulnerability or food defense concern, but that there is no evidence of product adulteration, they are to record the procedure, as performed, by recording trend indicator “S” and are to:

a. immediately notify the facility management and discuss the findings;

b. complete FSIS Form 5420-4, Food Defense Memorandum of Interview in PBIS; and

c. provide a copy to establishment management.

3. When import inspectors perform an 08S procedure and find that there is a food defense vulnerability or food defense concern, and that there is evidence of product adulteration, they are to record the procedure as performed by recording trend indicator “T” and are to:

a. immediately notify the facility management and discuss the findings and take action as per established policy;

b. complete a Noncompliance Record (NR) for the product adulteration and cite the appropriate ISP code and regulations;

c. complete FSIS 5420-4 in PBIS; and,

d. provide a copy of the forms to facility management.

4. When trend indicators “S” or “T” are entered in PBIS, the Vulnerability Report section of the screen is activated. Once this screen is activated, inspection personnel are to:

a. Click on the down arrow next to the Occurrence field and select:

i. “1 (First)”, if this is the first occurrence of this vulnerability,

ii. “2 (second)”, if this is the second occurrence, or

iii. “3 (3rd or more)”, indicating the third or more occurrence.

NOTE: For a finding to be reported as the second or third occurrence of a vulnerability, it must be for the same vulnerability under the performed 08 food defense procedure as occurred previously.

b. Verify that name of the inspector that performed the procedure appears in the Inspector field. To change the name:

i. click the magnifying glass icon next to the name field to open the Change Name Window;

ii. enter the inspector’s full name or partial name in the fields provided and click the Change Name button;

iii. select the appropriate name from the list and click the Select button.

c. Select applicable vulnerabilities by clicking the box adjacent to the vulnerability statement.

d. Record the management’s response in the Est. Mgmt Response section.

e. Review the information entered, make changes if necessary, and then click Save.

5. Inspection personnel are responsible for providing plant management a copy of the completed Form 5420-4, Food Defense Memorandum of Interview. To print FSIS Form 5420-4 in PBIS, inspection personnel may:

a. Print from the Procedure Results screen by highlighting the appropriate 08 Procedure and click the Print button; or

b. Print from the PBIS pull down menu;

i. select Reports / Results / Vulnerability Report;

ii. select the date range;

iii. select the establishment/shift then click Ok;

iv. a new window appears, select one or more vulnerability reports from the list and click Ok, then;

v. select the report destination. Enter S for screen, P for printer, or R for an RTF file then click OK.

B. The import facility is not under any regulatory obligation to respond. After meeting with facility management and completing FSIS Form 5420-4, import personnel do not need to verify how the import facility addressed the situation. Import personnel are to continue the random selection of food defense procedures.

C. If import inspection personnel, while randomly conducting food defense procedures, encounter a second occurrence of a potential food defense vulnerability or concern, they are to meet with the establishment management and complete a second MOI on the repeat vulnerability. Import inspection personnel are to note on the MOI that this is the second occurrence of this vulnerability.

NOTE: As stated above, the occurrence must be for the same vulnerability under the performed 08S sub-procedure.

D. If import inspection personnel, through the random performance of food defense procedures, encounter the potential food defense vulnerability or concern for a third time, they are to meet once again with the establishment management, complete a third MOI, and note on the MOI that it is the third occurrence of this vulnerability.

E. If the establishment expresses no intention to address the vulnerability or concern, import inspection personnel are to notify the Regional Import Field Supervisor (RIFO) of this situation through the Regional Supervisor. Import inspection personnel are not to further review or document the specific potential vulnerability identified in the three repeat MOIs until the RIFO provides further instructions. If the procedure is randomly selected, import inspection personnel are to direct verification procedures to establishment activities other than the one identified in the third MOI.

F. The RIFO is to request that OFDER conduct an assessment of the repeat findings.

G. OFDER's assessment is to include:

1. a review of the results of the Food Defense Plan Survey to determine whether the establishment has a functional food defense plan in place;

2. an assessment of the level of concern that the repeat findings present; and

3. a determination as to whether the establishment has been afforded sufficient time to mitigate the vulnerability.

H. OFDER is to provide the RIFO with the results of its assessment. The results may be:

1. that, because of the nature of the vulnerability, no specific action by the Agency is needed; or

2. that the establishment should be provided with specific guidance on how it can address the vulnerability.

I. In situations involving the latter assessment (H. 2. above), the RIFO is to forward OFDER's recommendation and the accompanying materials to import inspection personnel at the import establishment.

J. Import inspection personnel are to meet with the establishment management to discuss the vulnerability and how to address it more effectively. Import inspection personnel are to present to the establishment the material forwarded by OFDER. Import inspection personnel are to document what was discussed at this meeting on the third MOI.

K. Import inspection personnel are to provide a copy of the third MOI and the discussion notes to the RIFO. The RIFO is to forward a copy to the IF-OFDER mailbox.

XIII. ANALYSIS OF THE DATA

OFDER will analyze the food defense surveillance procedure information submitted to the ICS and PBIS systems on a monthly basis. The data will be analyzed for significant trends of food defense vulnerabilities where additional guidance or countermeasures can be directed. The analysis will also identify positive trends that can be shared with all agri-business stakeholders. OFDER will collaborate with OPEER and OIA if further analyses are needed.

Direct all questions related to this directive through supervisory channels.

Assistant Administrator
Office of Policy and Program Development